

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

UNITED STATES OF AMERICA

v.

ZACHARY BUCHTA, a/k/a “pein,”
“@fbiarelosers,” “@xotehpoodle,” and
“lizard”

16 CR 622

Judge Manish S. Shah

Government’s Sentencing Memorandum

Defendant Zachary Buchta was a prominent member of the hacking groups Lizard Squad and PoodleCorp. Through these groups, defendant caused hundreds of thousands of dollars in economic harm to the online gaming companies he targeted, and victimized countless others through the attack-for-hire website he operated. Following his arrest, however, defendant cooperated fully and truthfully with law enforcement. Pursuant to Guideline § 5K1.1 and the plea agreement in this case, the government recommends a sentence of 66% of the low end of the advisory guideline range, which works out to two-and-a-half years of imprisonment.

I. SUMMARY OF FACTS

As set forth in the PSR and criminal complaint, the defendant was a prominent member of hacking groups that launched a series of denial-of-service attacks against major computer gaming companies. The defendant also helped the groups run websites that allowed individuals to launch these attacks for hire against the targets of their choice. Defendant promoted these illegal activities through a variety of Twitter accounts, including “@pein,” “@fbiarelosers,” “@xotehpoodle,” and “@PoodleCorp.”

For example, on April 13, 2016, the “@LizardLands” twitter account promoted a DDOS attack by LizardSquad against Victim B, a major online game company. The account tweeted, “EU [Victim B] #Offline – [Victim B game #1] #Offline, [Victim B game #2] #Offline, [Victim B game #3] #Offline, [Victim B game #4] #Offline @fbiarelosers @AppleJ4ckxoxo,” “Arrest us,” and “More to come.” These tweets were retweeted by the defendant using the “@fbiarelosers” Twitter handle. Defendant participated in the attack and provided login credentials to another conspirator involved in the attack. R. 1, ¶¶ 44-49.

Defendant and his co-conspirators also engaged in other hacking activities to promote their hacking groups. For example, PoodleCorp claimed credit for compromising a YouTube channel operated by Victim S with more than 12 million listed subscribers. All of the posted videos visible in Victim S’s channel were changed to have the title “HACKED BY OBNOXIOUS AND PEIN twitter.com/poodlecorp.” The video also displayed a tweet from Victim S’s Twitter account made on June 22, 2016, which stated “HACKED BY @fbiarelosers and @BLADER.” R. 1, ¶¶ 55-56.

Defendant’s crime was a sophisticated one. Some of his coconspirators were located overseas, as was the computer server used to host the Shenron website. Defendant also used various means to attempt to hide his identity online.

II. OBJECTIONS, CORRECTIONS, AND CLARIFICATIONS TO THE PRESENTENCE INVESTIGATION REPORT

None.

III. GOVERNMENT’S ADVISORY GUIDELINE CALCULATION

The government agrees with the advisory guideline calculation set forth in the PSR. Defendant has a total offense level of 23 and a criminal history category of I, which results in an advisory guideline range of 46 to 57 months of imprisonment.

IV. THE FACTORS SET FORTH IN 18 U.S.C. § 3553(A) WARRANT A SENTENCE OF AT LEAST 108 MONTHS OF IMPRISONMENT

A. Nature and Circumstances of the Offense and the History and Characteristics of the Defendant

Defendant’s crime is serious. The online gaming companies targeted by the defendant suffered significant economic harm. It is impossible to calculate the harm to the thousands of victims affected by the Shenron and PoodleStresser services. These services relied on a massive network of compromised computers to launch their attacks. Defendant promoted these activities, encouraging others to engage in similar destructive behavior online. By tweeting messages such as “Arrest us” and “You can’t arrest a lizard” (and using the moniker “@fbiarelosers”), defendant encouraged others to believe such computer crimes could be committed with impunity.

There are also aspects of defendant’s history and characteristics that are troubling. While he has no criminal history, defendant did have prior contact with the FBI as far back as July 2014 with regard to different investigation into DDOS attacks.¹ That interview did little to deter defendant from continuing to engage in computer crimes. All of the conduct in this case followed that prior contact with law enforcement.

¹ Defendant was 17 years old at the time of the prior interview.

In mitigation, as set forth in more detail in the PSR, defendant faced some very difficult circumstances in childhood and appears to have made genuine efforts to turn his life around following his arrest in this case by obtaining employment and participating in mental health treatment. Defendant promptly admitted his conduct once he was charged in this case and cooperated with law enforcement after his arrest.

B. The Need to Reflect the Seriousness of the Offense, Promote Respect for the Law, Provide Just Punishment, Afford Adequate Deterrence, Protect the Public, and Provide Correctional Treatment

As discussed above, defendant's crime is a serious one. A sentence of imprisonment is important to reflect the seriousness of the offense and promote respect for the law.

A prison sentence is also needed to provide adequate deterrence. As set forth above, defendant and his coconspirators operated with a sense of impunity. Others who might be tempted to commit computer crimes need to know that they face serious consequences if caught. That is particularly true given defendant's contact with law enforcement as a juvenile. It is not uncommon for individuals engaged in computer crimes to first come to the attention of law enforcement as juveniles. It is important for the defendant and others to know that despite the leniency they may have received as juveniles, continuing to engage in computer crime as an adult will lead to significant penalties.

A sentence of 30 months' imprisonment will accomplish these purposes of punishment while being no greater than necessary to achieve them.

C. The Importance of the Guidelines and the Need to Avoid Unwarranted Sentencing Disparities

Although the Sentencing Guidelines are advisory only, “[a]s a matter of administration and to secure nationwide consistency, the Guidelines should be the starting point and the initial benchmark.” *Gall v. United States*, 522 U.S. 38, 49 (2007). For two reasons, this court should give serious consideration to the advisory Guidelines range. First, the Sentencing Guidelines are the sole factor in § 3553(a) that provides any objective sentencing range that can practicably promote the overall goal of minimizing unwarranted sentencing disparities, which is itself a statutorily-mandated factor, § 3553(a)(6). Second, the Guidelines generally deserve serious consideration because they are “the product of careful study based on extensive empirical evidence derived from the review of thousands of individual sentencing decisions.” *Gall*, 522 at 46.

While the government is recommending a below-guideline sentence in this case, that sentence is based on defendant’s substantial assistance to the government, as contemplated by Guideline § 5K1.1.

V. SUPERVISED RELEASE

The government agrees with the conditions of supervised release recommended by the probation officer.

VI. CONCLUSION

For the reasons set forth above, the government respectfully requests that defendant Zachary Buchta be sentenced to a term of imprisonment of 30 months.

Respectfully submitted,

JOHN R. LAUSCH, JR.
United States Attorney

By: s/Rajnath P. Laud
RAJNATH P. LAUD
Assistant United States Attorney
219 South Dearborn Street
Chicago, Illinois 60604
(312) 469-6306

Dated: March 13, 2018